MC

0500 #3

05-03-01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature: Lisa M. Hanlin Date: April 23, 2001

Applicant(s):	Philip D. MacKenzie
Case:	9
Serial No.:	09/827,227
Filing Date:	April 5, 2001
Title:	Methods and Apparatus for Providing Efficient Password-Authenticated Key Exchange
Group:	To Be Assigned
Examiner:	To Be Assigned

INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Pursuant to 37 C.F.R. §§1.56, 1.97 and 1.98, Applicant's attorney wishes to bring to the attention of the Patent and Trademark Office the following documents listed on the accompanying Form PTO-1449. A copy of each listed document is enclosed.

U.S. Patents

U.S. Patent No. 5,440,635 issued on 08/08/95 to Bellovin et al.

U.S. Patent No. 5,241,599 issued on 08/31/93 to Bellovin et al.

U.S. Patent Documents

U.S. Patent Application Serial No. 09/638,320, filed August 14, 2000 in the name of inventors V.V. Boyko et al. and entitled "Secure Mutual Network Authentication and Key Exchange Protocol."

U.S. Patent Application Serial No. 09/353,468, filed July 13, 1999 in the name of inventors P.D. MacKenzie et al. and entitled "Secure Mutual Network Authentication Protocol (SNAPI)."

Other Documents

1. D. Jablon, "Strong Password-Only Authenticated Key Exchange," ACM Computer Communications Review, ACM SIGCOMM, pp. 1-22, 1996.

2. S.M. Bellovin et al., "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 72-84, 1992.

3. S.M. Bellovin et al., "Augmented Encrypted Key Exchange: A Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise," Proceedings of the First Annual Conference on Computer and Communications Security, pages 1-7, 1993.

4. M. Steiner et al., "Refinement and Extension of Encrypted Key Exchange," ACM Operating System Review, pp. 1-9, 1994.

5. T. Wu, "The Secure Remote Password Protocol," Proceedings of the 1998 Internet Society Symposium on Network and Distributed System Security, pages 1-17, 1997.

6. Stefan Lucks, "Open Key Exchange: How to Defeat Dictionary Attacks Without Encrypting Public Keys," Security Protocol Workshop, pp. 1-12, 1997.

7. M. Bellare et al., "Authenticated Key Exchange Secure Against Dictionary Attacks," Advances in Cryptology, pp. 1-16, Eurocrypt 2000.

8. S. Patel, "Number Theoretic Attacks on Secure Password Schemes," Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 236-247, 1997.

9. W. Diffie et al., "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT 22, No. 6, pp. 644-654, 1976.

10. FIPS 180-1, "Secure Hash Standard," Federal Information Processing Standards Publication 180-1, pp. 1-21, 1995.

11. H. Dobbertin et al., RIPEMD-160: a Strengthened Version of RIPEMD, Fast Software Encryption, 3rd Intl. Workshop, pp. 1-13, 1996.

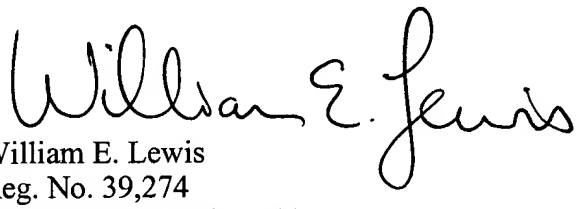
12. R.L. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.

13. D.P. Jablon, "Extended Password Key Exchange Protocols Immune to Dictionary Attack," WETICE Workshop on Enterprise Security, pp. 1-8, 1997.

It is believed that there is no fee due in conjunction with the filing of this Information Disclosure Statement. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Lucent Technologies Deposit Account No. 12-2325** as required to correct the error.

The filing of this Information Disclosure Statement shall not be construed as a representation that a search has been made, or as an admission that the information cited is considered to be material to patentability, or as a representation that no other material information exists.

Respectfully submitted,



William E. Lewis
Reg. No. 39,274
Attorney for Applicant(s)

Date: April 23, 2001
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, New York 11560
(516) 759-2946